



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/688,051	10/16/2003	Ammar Rayes	50325-0800	9185

29989 7590 11/15/2005

HICKMAN PALERMO TRUONG & BECKER, LLP  
2055 GATEWAY PLACE  
SUITE 550  
SAN JOSE, CA 95110

EXAMINER

TRAN, TONGOC

ART UNIT PAPER NUMBER

2134

DATE MAILED: 11/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b> 10/688,051	<b>Applicant(s)</b> RAYES ET AL	
	<b>Examiner</b> Tongoc Tran	<b>Art Unit</b> 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 16 October 2003.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-28 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-28 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)  | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date <u>10/16/2003</u> . | 6) <input type="checkbox"/> Other: _____  |

### **DETAILED ACTION**

1. This office action is in response to Applicant's application serial no. 10/688,051.

Claims 1-28 are pending.

### ***Information Disclosure Statement***

2. The information disclosure statement (IDS) submitted on March 17, 2004 has been considered by the Examiner.

### ***Claim Rejections - 35 USC § 101***

3. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 9-15 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The term "computer-readable medium" defines in the specification "may take many forms, including but not limited to, non-volatile media, volatile media, and transmission media ... Transmission media can also take the form of acoustic or light waves, such as those generated during radio wave and infrared data communications". A claim reciting a signal encoded with functional descriptive material does not fall within any of the categories of patentable subject matter set forth in 101. It is not a process because it is not a series of steps. It is not a machine because a claimed signal has no physical structure, does not itself perform any useful, concrete and tangible result and thus does not fit within the definition of a machine. It is not a composition of matter because a claimed signal is not a matter but a form of energy and

Art Unit: 2134

therefore is not a composition of matter. It is not a manufacture in accordance with dictionary definition to mean "the production of articles for use from raw or prepared materials by giving to these materials new forms, qualities, properties or combination, whether by hand-labor or by machinery." A claimed signal has no physical structure. These definitions require physical substance which a claimed signal does not have. It is not a manufacture because a manufacture is defined as the residual class of product. A product is a tangible physical article or object, some form of matter. Thus, a signal does not fall within one of the four statutory classes of 101.

***Claim Rejections - 35 USC § 112***

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 13, 14, and 26-28 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

In respect to claims 13, 14 and 27-28, Examiner finds wherein clause of the claimed limitation which recites "... wherein the information affecting the use of the network based on at least the health level is based on at least the course of action and is based on the health level as a result of being based on the course of action" (claim 13); "...wherein the information affecting the use of the network is based on at least the health level as a result of being is based on at least the user risk state, the current alert state, and the health state" (claims 14, and 26-28) to be unclear and confusing.

Furthermore, claims 14 and 26-28 also recite "determining a user risk state from a user risk level, determining a current alert state from a current alert level, and determining a health state from the health level" (claims 14 and 16); "calculating an alert state from an alert level...calculating a user risk state from a user risk level. However, on page 6 of the Specification, it states "[I]n this specification, the words, "level" and "state" are used interchangeably. Wherever one is used the other may be substituted". Examiner interprets this to mean the two terms are the same thing. Therefore, it is unclear what steps of determining or calculating Applicant intends to derive from the same element.

### ***Claim Rejections - 35 USC § 102***

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-12 and 15-25 rejected under 35 U.S.C. 102(e) as being anticipated by Proctor (U.S. Patent No. 6,530,024).

In respect to claim 1, Proctor discloses a policy-based network security management system, the system comprising: a security management controller comprising one or more processors; a computer-readable medium carrying one or more

sequences of instructions for policy-based network security management, wherein execution of the one or more sequences of instructions by the one or more processors causes the one or more processors to perform the steps of (see Abstract):  
receiving a set of data regarding a user of a network; automatically deciding on a course of action based on the set of data, wherein the course of action may be adverse to the user although the set of data is insufficient to establish whether the user is performing a malicious action; and sending signals to one or more network elements in the network to implement the decision (see col. 6, line 1 – col. 7, line 15).

In respect to claim 2, Proctor the system of claim 1, wherein the set of data includes at least one or more alerts related to the user (see col. 7, lines 5-15).

In respect to claim 3, Proctor discloses the system of claim 1, wherein the signals include multiple alerts generated by multiple users; and the system further comprising sequences of instructions for correlating the multiple alerts to the multiple users (see col. 7, lines 15-26).

In respect to claim 4, Proctor discloses the system of claim 1, wherein the set of data is a first set of data that is collected over a first duration of time; and the system further comprising sequences of instructions for collecting a second set of data over a second duration of time, wherein the first duration of time is shorter than the second duration of time (see col. 7, line 15-26).

In respect to claim 5, Proctor discloses the system of claim 4 further comprising sequences of instructions for performing the steps of:

assessing a risk level of the user harming the network based on the second set of data, wherein the second duration of time is sufficient to collect historical data regarding past malicious activities of the user (see col. 6, line 49-col. 7, line 4); and

assessing a current alert level based on the first set of data, wherein the first duration of time is of a length appropriate for assessing current activities of the user (see col. 7, lines 5-40).

In respect to claim 6, Proctor discloses the system of claim 1 or 5, further comprising sequences of instructions for performing the steps of: receiving signals related to an external source including at least an alert assessment relevant to the network as a whole; and creating and storing a current alert level value based on the alert assessment (see col. 6, line 25-col. 7, line 40).

In respect to claim 7, Proctor discloses the system of claim 1, further comprising sequences of instructions for performing the steps of:

receiving signals carrying performance information related to a health level of the network; and determining the course of action based at least in part on the set of data and the performance information (see col. 1, line 65-col. 2, line 50 and col. 6, line 49-col. 7, line 40).

In respect to claim 8, Proctor discloses the system of claim 1 further comprising:  
a plurality of routers for routing information sent by users and servers to a variety of destinations;

a subscriber management system for managing a network; a controller for executing the sequences of instructions; a network element for generating input for the set of data; and sequences of instructions for sending signals to the network elements (see col. 15, line 25-col. 17, line 10).

In respect to claim 9, Proctor discloses a computer-readable medium carrying one or more sequences of instructions for providing policy-based network security management, wherein execution of the one or more sequences of instructions by one or more processors causes the one or more processors to perform the steps of (see Abstract):

receiving signals carrying network performance information regarding health of a network and resource performance information regarding health of resources used by a network; assessing a health level based on the network performance information and the resource performance information; and sending signals carrying information affecting use of the network based on at least the health level (see Fig. 10, 11 and 13, col. 1, line 65-col. 2, line 5 and col. 5, line 61-col. 7, line 40).



In respect to claim 10, Proctor discloses a computer-readable medium as recited in claim 9, further comprising the steps of:

receiving signals related to one or more alerts; associating with the user at least the one or more alerts within a current alert dataset that establishes a current alert level for the user (see col. 6, line 52-col. 7, line 15).

In respect to claim 11, Proctor discloses a computer-readable medium as recited in claim 9, further comprising the step of establishing a user alert (see col. 7, lines 5-15).

In respect to claim 12, Proctor discloses the computer-readable medium as recited in claim 9, further comprising the steps of: receiving signals related to one or more alerts; associating with a user at least the one or more alerts within a historical dataset of alert related information that establishes a user risk level for the user (see col. 6, line 52-col. 7, line 15).

In respect to claim 15, the claimed limitation is similar to claim 9. Therefore, claim 15 is rejected based on the similar rationale.

In respect to claims 16-24, the claimed limitations are similar to claims 1-7 and 9. Therefore, claims 16-24 are rejected based on the similar rationale.

In respect to claim 25, Proctor discloses the method of claim 23, wherein the sending step further comprising the steps of :

Deciding on a course of action based on *at least* a user risk level, a current alert level, and the overall network health level, and the information affecting the use of the network includes at least information form carrying out the course of action ((see col. 6, line 52-col. 7, line 25).

### ***Conclusion***

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Peled et al. Disclose system and method for monitoring unauthorized transport of digital content.
- Yoon et al. Disclose alert transmission apparatus and method for policy based intrusion detection and response.
- Dettinger et al. Disclose an antiviral network system.
- Judge et al. Disclose system and method for adaptive message interrogation through multiple queues.
- Lim discloses a computer security event management system.
- Cantrell et al. Disclose an active network defense system and method.
- Wiegel discloses a graphical network security policy management.
- Gleichauf et al. Disclose a domain mapping method and system.


-Diep et al. disclose features generation for use in computer network intrusion detection.

-Scheidell discloses an intrusion detection system.

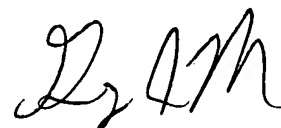
7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (571) 272-3843. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

  
Examiner: Tongoc Tran  
Art Unit: 2134

November 7, 2005



GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100